

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平 10 - 32567

(43) 公開日 平成 10 年 (1998) 2 月 3 日

(51) Int. Cl.	識別記号	庁内整理番号	F I	技術表示箇所
H04L 9/08			H04L 9/00	601 B
H04H 1/00			H04H 1/00	F
H04L 9/14			H04L 9/00	601 E
H04N 7/167				641
			H04N 7/167	Z
審査請求 未請求 請求項の数 3 O L (全 11 頁)				

(21) 出願番号 特願平 8 - 189636

(22) 出願日 平成 8 年 (1996) 7 月 18 日

(71) 出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目 2 番 3 号

(72) 発明者 秋田 康貴

東京都千代田区丸の内二丁目 2 番 3 号 三

菱電機株式会社内

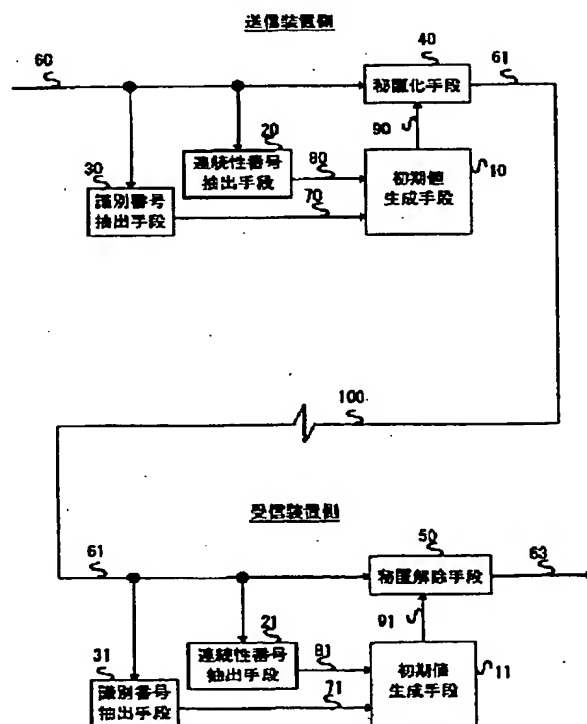
(74) 代理人 弁理士 宮田 金雄 (外 3 名)

(54) 【発明の名称】 秘匿化装置、秘匿解除装置およびこれらを用いたデータ伝送システム

(57) 【要約】

【課題】 送信装置と受信装置間で、メディアデータを秘匿化して送信するシステムで第 3 者に視聴されない秘匿強度の高いシステムを得る。

【解決手段】 送信装置においては、連続性番号抽出手段 20、識別番号抽出手段 30 でバケット 60 のヘッダ領域からメディアデータ連続性番号、識別番号の特定情報を抽出し、これらにより初期値生成手段 10 で初期値を生成し、この初期値により秘匿化手段 40 で送信バケット 60 の情報領域を秘匿化する。受信側装置は、受信バケット 61 のヘッダ領域から連続性番号と識別番号を連続性番号抽出手段 21、識別番号抽出手段 31 で抽出する。これらにより初期値生成手段 11 で初期値を生成し、この初期値により秘匿解除手段 50 で受信バケットの秘匿化された情報領域の秘匿解除を行なう。



【特許請求の範囲】

【請求項 1】 ヘッダ領域と情報領域とを有するパケットの情報領域に格納されるデータを秘匿化してパケットを送信する秘匿化装置であって、

前記パケットのヘッダ領域の特定情報を抽出する抽出手段と、前記抽出された特定情報に基づいて初期値を生成する初期値生成手段と、

前記初期値生成手段により生成された初期値に基づいて予め定められたアルゴリズムにより前記パケットの情報領域のデータを秘匿化する秘匿化手段とを備えたことを特徴とする秘匿化装置。

【請求項 2】 ヘッダ領域と情報領域とを有するパケットの情報領域のデータが所定のアルゴリズムで秘匿化されたパケットの秘匿解除処理を行い復元したパケットを出力する秘匿解除装置であって、

前記受信パケットのヘッダ領域の特定情報を抽出する抽出手段と、

前記抽出された特定情報に基づいて初期値を生成する初期値生成手段と、

前記初期値生成手段により生成された初期値に基づいて所定のアルゴリズムにより前記パケットの情報領域の秘匿化データの秘匿解除を行ない復元パケットを出力する秘匿解除手段、

とを備えたことを特徴とする秘匿解除装置。

【請求項 3】 ヘッダ領域と情報領域を有するパケットの情報領域に格納されるデータを秘匿化して送受信するデータ通信システムであって、

送信側装置は、送信パケットのヘッダ領域の特定情報を抽出する第 1 の抽出手段と、前記第 1 の抽出手段により抽出された特定情報に基づいて送信パケットの情報領域のデータを秘匿化するための初期値を生成する第 1 の初期値生成手段と、前記第 1 の初期値生成手段により生成された初期値に基づいて前記パケットの情報領域のデータを秘匿化しパケットを送信する秘匿化手段、

とを備え、

受信側装置では、受信パケットのヘッダ領域の特定情報を抽出する第 2 の抽出手段と、前記第 2 の抽出手段により抽出された特定情報に基づいて受信パケットの情報領域の秘匿化されたデータを解除するための初期値を生成する第 2 の初期値生成手段と、

前記第 2 の初期値生成手段により生成された初期値に基づいて受信パケットの情報領域の秘匿化されたデータを解除し復元パケットを出力する解除手段とを備えたことを特徴とするデータ伝送システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、メディアデータなどの送信データをパケット化し、パケット化されたデータに秘匿化を行ったパケットを送信装置から受信装置に伝送する場合に用いられ、第三者によるデータの内容

の傍受を回避するためにデータを秘匿化する秘匿化装置と秘匿化されたデータを解除する秘匿解除装置およびこれらを用いたデータ伝送システムに関するものである。

【0002】

【従来の技術】近年伝送路の高帯域化や高能率圧縮符号化方式が進展してきたことにより、映像や音声等のメディアデータを効率的に伝送するデータ通信が普及してきた。企業内におけるテレビ会議システムや有料放送システム等の導入がその代表例である。一方、これらのシステムの導入が普及するにつれて第三者による社外秘情報の傍受や、非加入者による有料放送の不正視聴などの可能性も高まっている。このような事態を回避するために、特定の秘匿化アルゴリズムによりメディアデータを送信装置側で秘匿化し、受信装置側で秘匿化されたメディアデータを秘匿解除して元のメディアデータに復元することが一般的となってきた。

【0003】メディアデータの伝送、特にリアルタイム性が要求される映像とこれに付随する音声の伝送においてデータの秘匿化を行う場合には、秘匿化すべき各メディアデータを適当な長さに区切ってブロック化し、ブロック単位で秘匿化し、秘匿化処理を開始する毎に所定の初期値を用いることにより、万一伝送路上において秘匿化ブロック内でビット誤りが発生してもその誤りが他の秘匿化ブロックに波及しないようにし、秘匿解除が不可能となるのがビット誤りの発生した特定の秘匿化ブロックだけとなるようにするのが一般的である。図 9 は、例えば「64 ビットのブロック暗号アルゴリズムの利用モード」(JIS X 5052、ISO 8372)で示されている CBC (Cipher Block Chaining) モードの動作を説明する図である。図中、暗号化処理部は請求項 1 に記載の秘匿化手段に相当する。また復号処理部は請求項 2 に記載の秘匿解除手段に相当する。このモードでは、暗号化処理の過程で暗号文を平文側にフィードバックする。E_i を鍵 K による暗号化、D_i を鍵 K による復号、C_i を初期値、P_i を平文 i、C_i を暗号文 i とすると、下記の式 (1) のように表わせる。

【0004】

【数 1】

$$\begin{aligned} C_i &= E_k(P_i \oplus C_{i-1}) \\ P_i &= D_k(C_i) \oplus C_{i-1} \end{aligned}$$

⊕…排他論理和

【0005】初期値 C₁ は、ブロック化されたデータを暗号化処理するための最初の入力値である。鍵が同じでも初期値を変更すると同じ平文から異なる暗号文を生成することができる。従って、ブロック単位に初期値を変更すれば、暗号強度を高めることができる。

【0006】図 8 は、特開昭 63-167588 号公報

3

に示された従来の秘匿化データ伝送システムである。図において、伝送データ処理手段 2 1 1 は映像信号 2 1 0 を入力して秘匿化を行う回路であり、同処理手段 2 1 1 の出力はデータ重畳手段 2 1 2 を介して伝送路 2 1 3 に導かれる。映像信号 2 1 0 は伝送回数制御手段 2 1 4 にも供給されている。伝送回数制御手段 2 1 4 は映像信号 2 1 0 の垂直同期信号をカウントして信号 2 1 4 a、2 1 4 b、2 1 4 c を出力している。このうち信号 2 1 4 a は垂直同期信号がカウントされる毎にインクリメントする信号であり、初期値変換手段 2 1 6 に入力される。伝送回数制御手段 2 1 4 の出力信号 2 1 4 b、2 1 4 c は、初期値 2 1 5 a を変更するタイミングを与える信号であり、例えば n フィールド毎に初期値を変更する場合、伝送回数制御手段 2 1 4 の最大カウント値が n に設定され、このとき信号 2 1 4 b はカウント値 n に対応して出力される。これにより n カウント出力 2 1 4 b のタイミングで新たな初期値 2 1 5 a が発生され、重畳データ作成手段 2 1 7 は n カウント出力時に同期パターン発生手段 2 1 8 の出力を選択し、それ以外の期間に初期値 2 1 5 a を選択する。なお初期値発生手段 2 1 5 はカウント値 n から次カウント周期の n - 1 まで新たな初期値 2 1 5 a を維持している。

【0 0 0 7】一方、初期値変換手段 2 1 6 は、上記の新たな初期値 2 1 5 a が初期値発生手段 2 1 5 より発生するタイミングで以前に発生していた初期値 2 1 5 a を n フィールド期間ラッチ出力する機能を有しており、このラッチ出力された以前の初期値は、信号 2 1 4 a の各インクリメント値で所定の論理変換を受け、その変換データに基づく乱数信号 2 1 6 a を発生する。そしてこの出力する乱数信号 2 1 6 a のタイミングで伝送データ処理手段 2 1 1 に入力した映像信号を秘匿化する。なお本従来例では映像のフィールド単位が秘匿化すべきデータのブロック単位となっていることは明らかである。

【0 0 0 8】こうして伝送路 2 1 3 には上記変換データを初期値として秘匿化された映像信号 2 2 5 が伝送される。伝送路 2 1 3 からの秘匿化映像信号 2 1 9 は、受信データ処理手段 2 2 0、データ抽出手段 2 2 1 及び伝送回数カウント手段 2 2 2 に供給されている。受信データ処理手段 2 2 0 は送信装置側における伝送データ処理手段 2 1 1 と逆の処理を行い、秘匿化映像信号 2 1 9 を秘匿解除する回路である。また、データ抽出手段 2 2 1 は所定期間に重畳された初期値を各フィールド毎すべて抽出する回路である。伝送回数カウント手段 2 2 2 は秘匿化映像信号 2 1 9 における垂直同期信号をカウントし、そのカウント出力 2 2 2 a を初期値変換手段 2 2 3 に供給する。この場合、伝送回数カウント手段 2 2 2 は、同期パターンを検索する同期パターン検出手段 2 2 4 が同期パターンを検出すると、そのタイミングを示す信号 2 2 4 a によってカウンタ値がクリアされる。これにより初期値変換手段 2 2 3 は送信装置側と同一の乱数

4

信号 2 2 3 a を出力することになり、受信データ処理手段 2 2 0 からは正確に秘匿解除された映像信号 2 2 6 が出力される。

【0 0 0 9】

【発明が解決しようとする課題】従来の秘匿化データ伝送システムは以上のように構成されており、n フィールド毎に初期値を変更し、さらに所定の論理変換を行った初期値を伝送する。しかし所定の論理変換を行っているとはいえ、伝送路上に初期値が出現するのであり、第三者によりこの初期値が解読され、伝送される秘匿化データが秘匿解除されて不正に視聴される場合があるという問題点があった。本発明は上記のような問題点を解消するためになされたもので、送信装置と受信装置間で初期値を伝送せずに秘匿化処理を実現するとともに、秘匿化すべきデータを適当な長さに区切ってブロック化、すなわちバケット化し、各バケットの秘匿化処理を開始する毎に所定の初期値を用いることにより、秘匿強度を高めた秘匿化データ伝送システムを得ることを目的とする。

【0 0 1 0】

【課題を解決するための手段】この発明の第 1 の発明は、ヘッダ領域と情報領域とを有するバケットの情報領域に格納されるデータを秘匿化してバケットを送信する秘匿化装置であって、前記バケットのヘッダ領域の特定情報を抽出する抽出手段と、前記抽出された特定情報に基づいて初期値を生成する初期値生成手段と、前記初期値生成手段により生成された初期値に基づいて予め定められたアルゴリズムにより前記バケットの情報領域のデータを秘匿化する秘匿化手段を備える。

【0 0 1 1】この発明の第 2 の発明は、ヘッダ領域と情報領域とを有するバケットの情報領域が所定のアルゴリズムで秘匿化されたバケットの秘匿解除処理を行い復元したバケットを出力する秘匿解除装置であって、前記受信バケットのヘッダ領域の特定情報を抽出する抽出手段と、前記抽出された特定情報に基づいて初期値を生成する初期値生成手段と、前記初期値生成手段により生成された初期値に基づいて所定のアルゴリズムにより前記バケットの情報領域の秘匿化データの秘匿解除を行ない復元バケットを出力する秘匿解除手段を備える。

【0 0 1 2】この発明の第 3 の発明は、ヘッダ領域と情報領域とを有するバケットの情報領域に格納されるデータを秘匿化して送受信するデータ通信システムであって、送信側装置は、送信バケットのヘッダ領域の特定情報を抽出する第 1 の抽出手段と、前記第 1 の抽出手段により抽出された特定情報に基づいて送信バケットの情報領域のデータを秘匿化するための初期値を生成する第 1 の初期値生成手段と、前記第 1 の初期値生成手段により生成された初期値に基づいて前記バケットの情報領域のデータを秘匿化しバケットを送信する秘匿化手段、とを備え、受信側装置では、受信バケットのヘッダ領域の特定情報を抽出する第 2 の抽出手段と、前記第 2 の抽出手段

により抽出された特定情報に基づいて受信パケットの情報領域の秘匿化されたデータを解除するための初期値を生成する第 2 の初期値生成手段と、前記第 2 の初期値生成手段により生成された初期値に基づいて受信パケットの情報領域の秘匿化されたデータを解除し復元パケットを出力する解除手段を備える。

【0013】

【発明の実施の形態】

実施の形態 1. 以下、本発明の一実施の形態を図について説明する。図 1 は、本発明に係る秘匿化データ伝送システムの一実施の形態を示す図である。図 2 は、本発明に係る秘匿化データ伝送システムで伝送されるパケットの構成を示す図、図 3 は、秘匿化前及び秘匿解除後のパケットと秘匿化パケットの構成を示す図、図 4 は本発明に係るパケットの秘匿化処理と秘匿解除処理のタイミングチャートを示す図、図 5 は本発明に係る初期値生成手段の構成を示す図、図 6 は本発明に係る秘匿化手段の構成を示す図、図 7 は本発明に係る秘匿解除手段の構成を示す図である。なお、図 4 で示すタイミングチャートは本発明の動作説明用のものであり、厳密なタイミングを規定するものではない。

【0014】図 1 において、10 と 11 は初期値生成手段、20 と 21 は連続性番号抽出手段、30 と 31 は識別番号抽出手段である。40 は秘匿化手段、50 は秘匿解除手段、100 は伝送路である。60 は送信パケット、61 は秘匿化パケット、63 は秘匿解除パケットで送信パケット 60 と同一である。70 と 71 はメディアデータなどデータの種別を識別する識別番号で、パケットの情報領域に格納されたメディアデータなどのデータの種別に応じてユニークに割り当てられた番号である。80 と 81 は連続性番号で、パケットを伝送する毎に所定の順序付け方法にて順序つけられた番号である。ここで、この実施の形態では、ヘッダ領域の連続番号と識別番号を特定情報とし、連続性番号抽出手段と識別番号抽出手段をヘッダ領域の特定情報を抽出する抽出手段とする。図 2 において、64 はパケットのヘッダ領域、65 はパケットの情報領域である。情報領域 65 にはメディアデータが格納される。ヘッダ領域 64 には、上述のメディアデータ識別番号と連続性番号とが格納される。図 3 において、(a) は秘匿化前または秘匿解除後のメディアデータを情報領域に格納したパケットの構成、(b) は秘匿化されたメディアデータを情報領域に格納したパケットの構成を示す。

【0015】送信装置において、送信パケット 60 が秘匿化パケット 61 として出力されるまでを図 1、図 4、図 5、図 6 を用いて説明する。送信パケット 60 は、識別番号抽出手段 30、連続性番号抽出手段 20 及び秘匿化手段 40 に供給されており、その構成は図 2 に示す通りである。識別番号抽出手段 30 は、メディアデータを情報領域に格納した送信パケット 60 を入力し、当該パ

ケットのヘッダ領域を検出し、当該メディアデータを識別するためにユニークに割り当てられたメディアデータ識別番号 70 をそのヘッダ領域から抽出して初期値生成手段 10 へ出力する。このとき識別番号抽出手段 30 は、図 4 の (a) に示すようにメディアデータ識別番号 70 を検出したら直ちに初期値生成手段 10 へ出力し、少なくとも送信パケット 60 の情報領域 65 が入力されるまで出力保持する機能を有する。

【0016】連続性番号抽出手段 20 は、識別番号抽出手段 30 に入力されるパケットと同一のパケット 60 を入力し、当該パケットのヘッダ領域を検出し、伝送されるパケットの連続性を示す連続性番号 80 をそのヘッダ領域から抽出して初期値生成手段 10 へ出力する。このとき連続性番号抽出手段 20 は、図 4 の (a) に示すように連続性番号 80 を検出したら直ちに初期値生成手段 10 へ出力し、少なくとも送信パケット 60 の情報領域 65 が入力されるまで出力保持する機能を有する。初期値生成手段 10 は、送信するパケットのメディアデータ識別番号 70 と連続性番号 80 とをそれぞれ識別番号抽出手段 30 と連続性番号抽出手段 20 とから入力し、これらのメディアデータ識別番号 70 と連続性番号 80 との組合わせを元にして当該パケットの情報領域に格納されるメディアデータを秘匿化するために必要な初期値 90 を生成して秘匿化手段 40 へ出力する。このとき初期値生成手段 10 は、図 4 の (a) に示すようにメディアデータ識別番号 70 と連続性番号 80 の両方が共に入力された時点で直ちに初期値 90 を生成して秘匿化手段 40 へ出力し、少なくとも送信パケット 60 の情報領域 65 が入力されるまで出力保持する機能を有する。

【0017】初期値生成手段 10 の構成例を図 5 に示す。メディアデータ識別番号 70 と連続性番号 80 は、次の入力があるまでそれぞれレジスタ 111 とレジスタ 112 に保持される。演算部 113 においては、レジスタ 111 とレジスタ 112 に保持されたメディアデータ識別番号 70 と連続性番号 80 とを入力して所定の方法で演算を実施し、複数の初期値 (図中、C01 ~ C0k) が格納されたメモリ 114 の特定のアドレスを生成する。このとき演算部 113 は、入力されるメディアデータ識別番号 70 と連続性番号 80 とに基づいて、加算、減算、乗算、除算のいずれかを使用した演算を実施する。メモリ 114 は、演算部 113 から与えられたアドレスに対応した初期値をその格納領域から読み出し、初期値 90 として出力する。

【0018】秘匿化手段 40 は、送信パケット 60 に対応した初期値 90 を初期値生成手段 10 から入力し、当該パケットの情報領域に格納されたメディアデータを秘匿化して秘匿化パケット 61 として出力する。このとき秘匿化手段 40 は、図 4 の (a) に示すように当該パケット 60 の情報領域 65 のメディアデータが入力される直前に初期値 90 をロードし、図 9 に示すような秘匿化

処理を情報領域 6 5 の最後のデータまで継続して実施する。なお、秘匿化手段 4 0 はヘッダ領域については秘匿化を行わないので、図 3 の (b) に示すように出力される秘匿化バケット 6 1 は秘匿化されないヘッダ領域と秘匿化された情報領域を持つ構成となる。

【 0 0 1 9 】秘匿化手段 4 0 の構成例を図 6 に示す。ヘッダ分離部 4 0 1 は、入力された送信バケット 6 0 からヘッダ領域 6 4 と情報領域 6 5 とを分離して、それぞれヘッダレジスタ 4 0 3 と秘匿化処理部 4 0 2 に出力する。秘匿化処理部 4 0 2 は、情報領域 6 5 に対し、与えられた初期値 9 0 を用いて秘匿化処理を実施する。ヘッダレジスタ 4 0 3 は、分離されたヘッダ領域 6 4 を一時的に保持する。ヘッダ付加部 4 0 4 は、秘匿化処理部 4 0 2 にて秘匿化処理が実施された情報領域 6 5 に対して、ヘッダレジスタ 4 0 3 にて一時的に保持されたヘッダ領域 6 4 を付加して、秘匿化バケット 6 1 として出力する。以上のようにして伝送路 1 0 0 には、情報領域が秘匿化された秘匿化バケット 6 1 が伝送される。

【 0 0 2 0 】受信装置において、秘匿化バケット 6 1 が秘匿解除されたバケット 6 3 として出力されるまでを図 1、図 4、図 5、図 7 を用いて説明する。伝送路 1 0 0 から入力する秘匿化バケット 6 1 は、識別番号抽出手段 3 1、連続性番号抽出手段 2 1 及び秘匿解除手段 5 0 に供給されており、その構成は図 2 に示す通りである。識別番号抽出手段 3 1 は、秘匿化バケット 6 1 を入力し、当該バケットのヘッダ領域を検出し、当該メディアデータ識別番号 7 1 をそのヘッダ領域から抽出して初期値生成手段 1 1 へ出力する。このとき識別番号抽出手段 3 1 は、図 4 の (b) に示すようにメディアデータ識別番号 7 1 を検出したら直ちに初期値生成手段 1 1 へ出力し、少なくとも秘匿化バケット 6 1 の情報領域 6 5 が入力されるまで出力保持する機能を有する。

【 0 0 2 1 】連続性番号抽出手段 2 1 は、識別番号抽出手段 3 1 に入力されるバケットと同一のバケット 6 1 を入力し、当該バケットのヘッダ領域を検出し、伝送されるバケットの連続性を示す連続性番号 8 1 をそのヘッダ領域から抽出して初期値生成手段 1 1 へ出力する。このとき連続性番号抽出手段 2 1 は、図 4 の (b) に示すように連続性番号 8 1 を検出したら直ちに初期値生成手段 1 1 へ出力し、少なくとも秘匿化バケット 6 1 の情報領域 6 5 が入力されるまで出力保持する機能を有する。初期値生成手段 1 1 は、受信した秘匿化バケット 6 1 のメディアデータ識別番号 7 1 と連続性番号 8 1 とをそれぞれ識別番号抽出手段 3 1 と連続性番号抽出手段 2 1 とから入力し、これらのメディアデータ識別番号 7 1 と連続性番号 8 1 との組合わせを元にして当該バケットの情報領域に格納されるメディアデータを秘匿解除するために必要な初期値 9 1 を生成して秘匿解除手段 5 0 へ出力する。このとき初期値生成手段 1 1 は、図 4 の (b) に示

すようにメディアデータ識別番号 7 1 と連続性番号 8 1 の両方が共に入力された時点で直ちに初期値 9 1 を生成して秘匿解除手段 5 0 へ出力し、少なくとも秘匿化バケット 6 1 の情報領域 6 5 が入力されるまで出力保持する機能を有する。初期値生成手段 1 1 の構成例は初期値生成手段 1 0 の構成例を示す図 5 と同様であり、その動作も同様であるので、説明は省略する。

【 0 0 2 2 】秘匿解除手段 5 0 は、受信した秘匿化バケット 6 1 に対応した初期値 9 1 を初期値生成手段 1 1 から入力し、当該バケットの情報領域に格納されたメディアデータを秘匿解除して元のバケット 6 3 に復元し、これを出力する。このとき秘匿解除手段 5 0 は、図 4 の (b) に示すように当該バケット 6 1 の情報領域 6 5 のメディアデータが入力される直前に初期値 9 1 をロードし、図 9 に示すような秘匿処理を情報領域 6 5 の最後のデータまで継続して実施する。秘匿解除手段 5 0 の構成例を図 7 に示す。ヘッダ分離部 5 0 1 は、入力された秘匿化バケット 6 1 からヘッダ領域 6 4 と秘匿化された情報領域 6 5 とを分離して、それぞれヘッダレジスタ 5 0 3 と秘匿解除処理部 5 0 2 に出力する。秘匿解除処理部 5 0 2 は、秘匿化された情報領域 6 5 に対し、与えられた初期値 9 1 を用いて秘匿解除処理を実施する。ヘッダレジスタ 5 0 3 は、分離されたヘッダ領域 6 4 を一時的に保持する。ヘッダ付加部 5 0 4 は、秘匿解除処理部 5 0 2 にて秘匿解除処理が実施された情報領域 6 5 に対して、ヘッダレジスタ 5 0 3 にて一時的に保持されたヘッダ領域 6 4 を付加して、秘匿解除バケット 6 3 として出力する。

【 0 0 2 3 】バケットの構成を示す図 2 についてさらに説明する。ヘッダ領域 6 4 は当該バケットの制御情報が格納される領域であり、制御情報の中には少なくともメディアデータ識別番号と連続性番号とが格納されている。情報領域 6 5 は、適当なデータ長に区切られたメディアデータが格納される領域である。なおひとつのバケットにおける情報領域に格納されるメディアデータは 1 種類である。メディアデータ識別番号は、送信装置側で付与され、情報領域 6 5 に格納されたメディアデータの種類の応じてユニークに割り当てられた識別番号であって、受信装置はこのメディアデータ識別番号を検出して当該バケットに格納されたメディアデータの種類の判断する。連続性番号は、送信装置側で付与され、バケットを伝送する毎に所定の順序付け方法にて順序付けられた番号であって、受信装置はこの連続性番号の連続性を監視することによって受信したバケットの損失の有無等を判断する。従ってメディアデータ識別番号と連続性番号は本来上述の処理を目的としたものであり、秘匿化処理のための情報ではないのであり、メディアデータ識別番号と連続性番号とを秘匿化処理及び秘匿解除処理に利用することが本発明の特徴である。

【 0 0 2 4 】図 3 の (a) は送信バケット 6 0 と秘匿解

除されたパケット 6 3 (即ち元の送信パケット 6 0) の構成を示し、(b) は秘匿化パケット 6 1 の構成を示している。(a) の構成の送信パケット 6 0 の情報領域のメディアデータが秘匿化手段 4 0 で秘匿化されると、

(b) の構成の秘匿化パケット 6 1 になる。このとき秘匿化処理の対象はパケットの情報領域だけであり、ヘッダ領域は秘匿化されない。一方、(b) の構成の秘匿化パケット 6 1 の情報領域のメディアデータは秘匿解除手段 5 0 で秘匿解除され、(a) の構成のパケット 6 3 となり、元の送信パケット 6 0 に復元される。

【0025】

【発明の効果】 以上のように本発明による秘匿化装置、秘匿解除装置およびこれらを用いたデータ伝送システムでは、送信装置と受信装置間で伝送路を経由して初期値を伝送しないので、第三者により初期値を傍受されることがなく、従って伝送される秘匿化データが第三者により秘匿解除されて不正視聴されることを防止することができる効果がある。また各パケットの秘匿化処理を開始する毎に所定の初期値を用いる構成としたので、秘匿強度をより一層高めることができる効果がある。

【図面の簡単な説明】

【図 1】 本発明に係る秘匿化データ伝送システムの構成を示す図である。

【図 2】 本発明に係る秘匿化データ伝送システムで伝送されるパケットの構成を示す図である。

【図 3】 本発明に係る秘匿化データ伝送システムにお

ける秘匿化前及び秘匿解除後のパケットと秘匿化パケットの構成を示す図である。

【図 4】 本発明に係る秘匿化データ伝送システムにおけるパケットの秘匿化処理と秘匿解除処理のタイミングチャートを示す図である。

【図 5】 本発明に係る秘匿化データ伝送システムにおける初期値生成手段の構成を説明するための図である。

【図 6】 本発明に係る秘匿化データ伝送システムにおける秘匿化手段の構成を説明するための図である。

10 【図 7】 本発明に係る秘匿化データ伝送システムにおける秘匿解除手段の構成を説明するための図である。

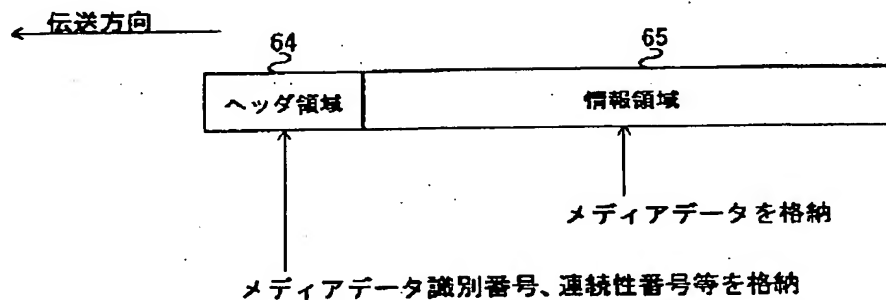
【図 8】 従来の秘匿化データ伝送システムの構成を示す図である。

【図 9】 「64 ビットのブロック暗号アルゴリズムの利用モード」(JIS X 5052、ISO 8372) で示されている CBC (Cipher Block Chaining) モードの動作を説明する図である。

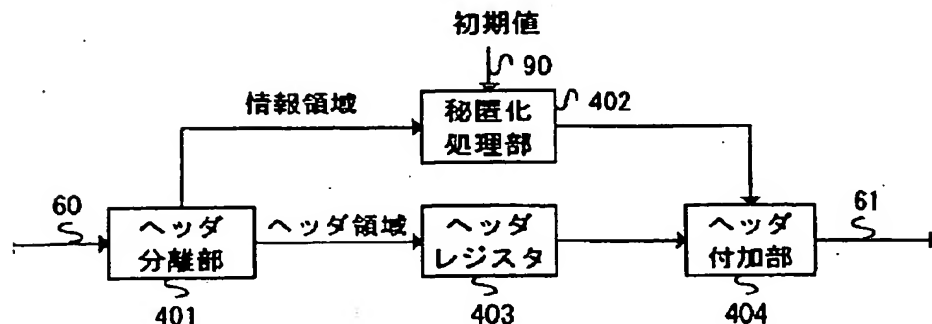
【符号の説明】

10、11 初期値生成手段、 20、21 連続性番号抽出手段、 30、31 識別番号抽出手段、 40 秘匿化手段、 50 秘匿解除手段、 60 送信パケット、 61 秘匿化パケット、 63 秘匿解除パケット、 64 ヘッダ領域、 65 情報領域、 70、71 メディアデータ識別番号、 80、81 連続性番号、 90、91 初期値、 100 伝送路。

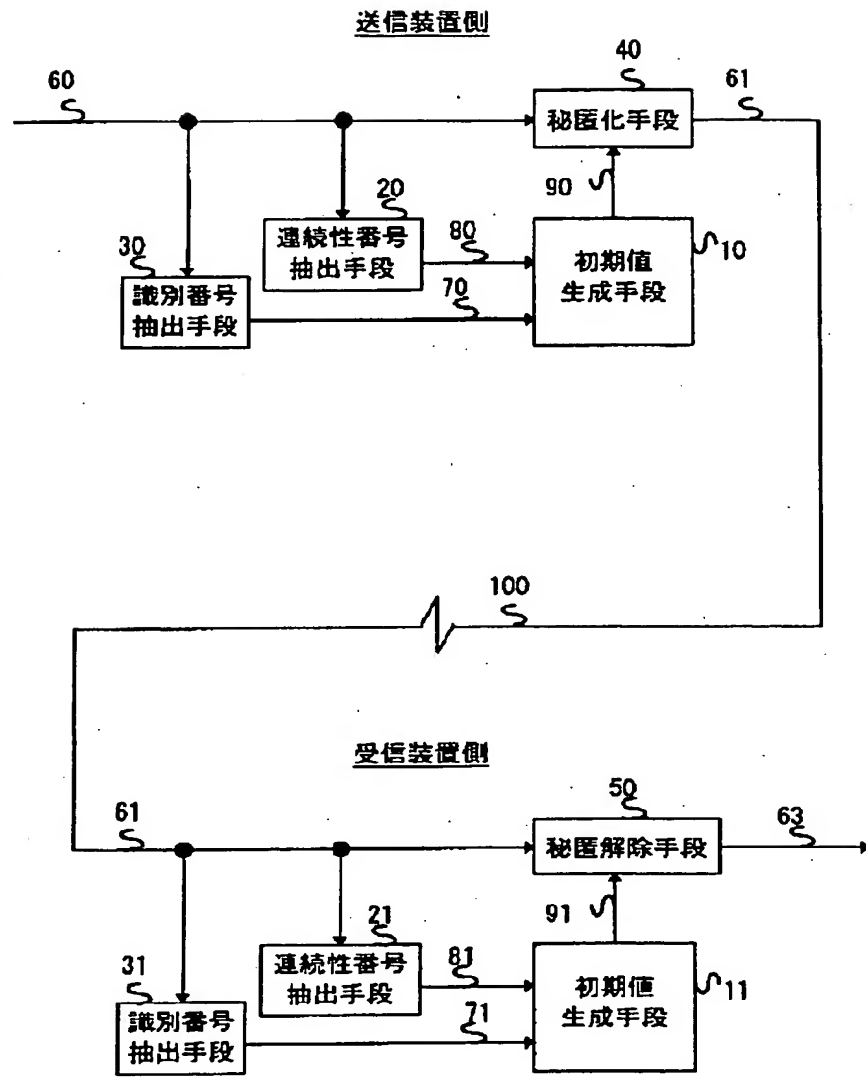
【図 2】



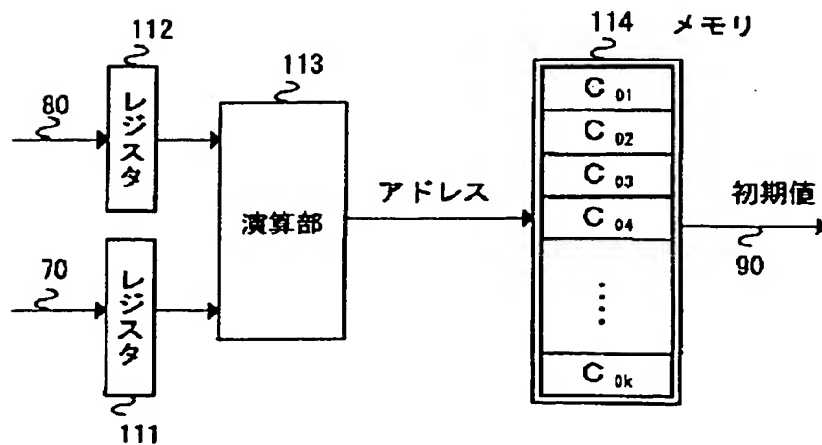
【図 6】



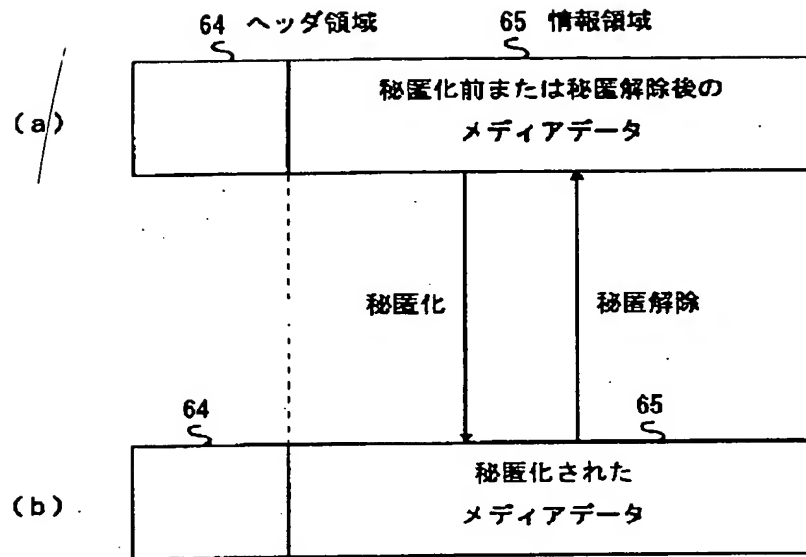
【図 1】



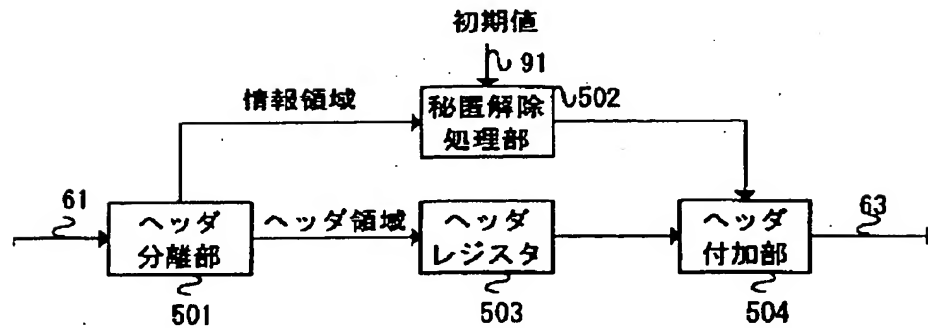
【図 5】



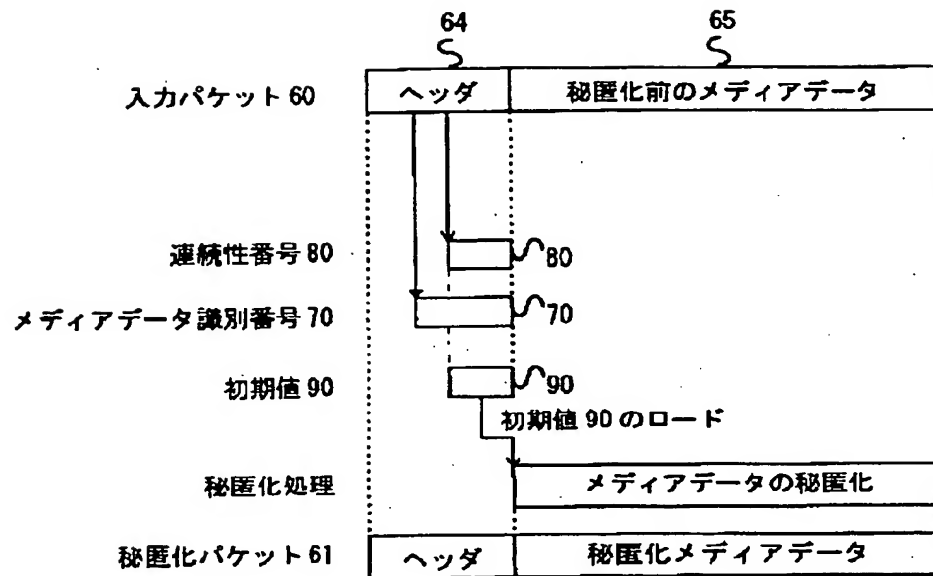
【図 3】



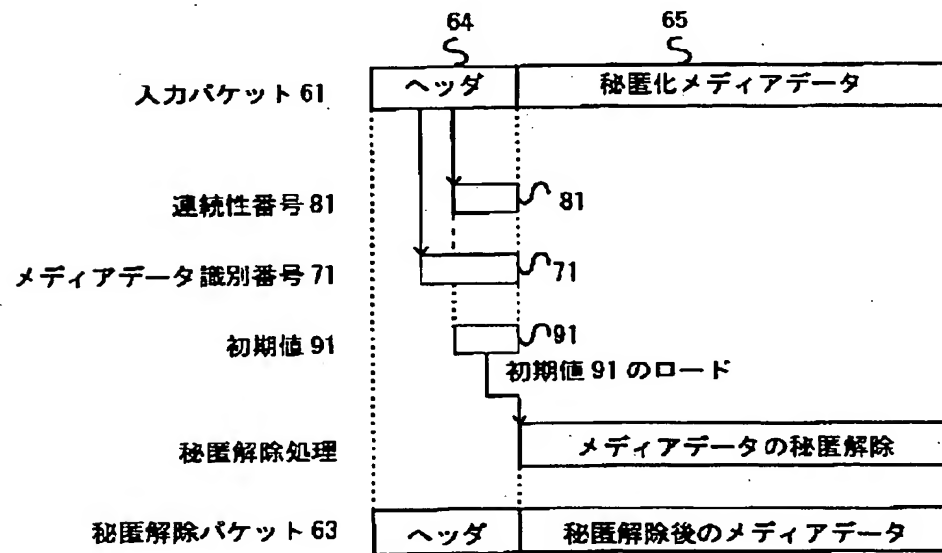
【図 7】



【図 4】



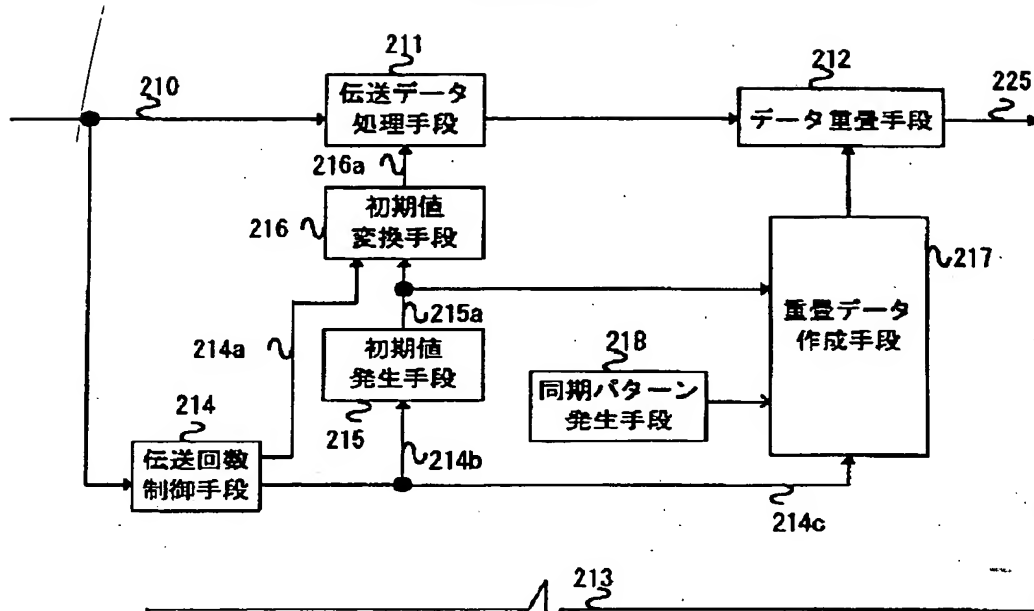
(a) 送信装置側におけるパケットの秘匿化処理タイミング



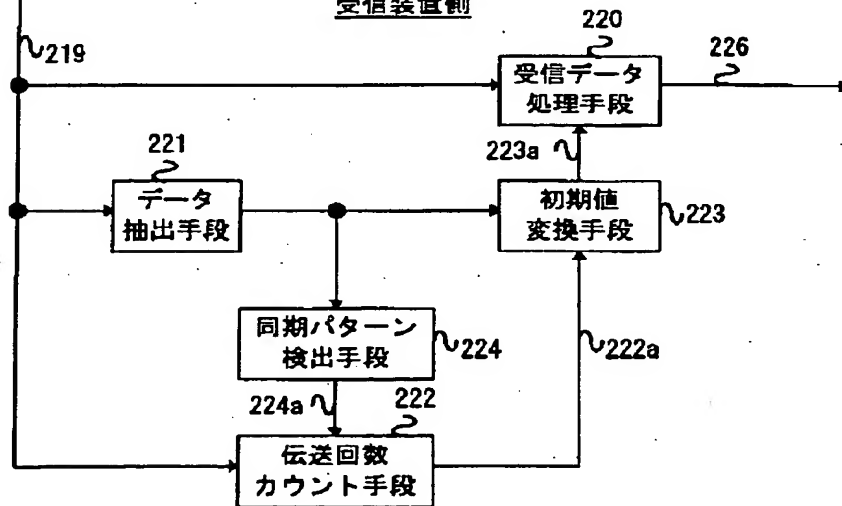
(b) 受信装置側におけるパケットの秘匿解除処理タイミング

【図 8】

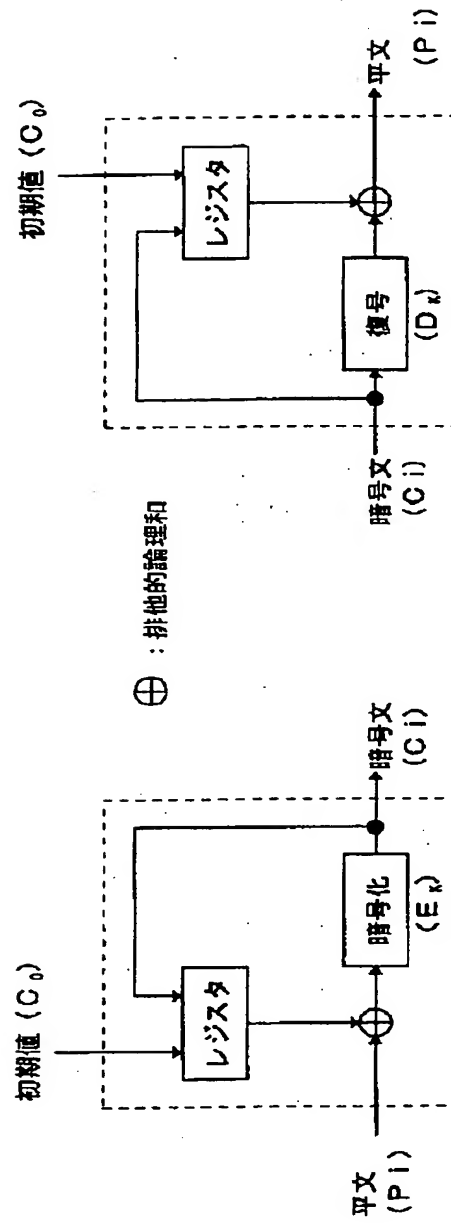
送信装置側



受信装置側



【図9】



(b) 復号処理部

(a) 暗号化処理部